

YASHIL

IQTISODIYOT va TARAQQIYOT

Ijtimoiy, iqtisodiy, texnologik, ilmiy, ommabop jurnal



ZAMONAVIY IQTISODIYOTDA YUQORI MUHANDISLIK TEKNOLOGIYALARINI ILMIY-AMALIY JORIY ETISH INNOVATSION TARAQQIYOT POYDEVORI

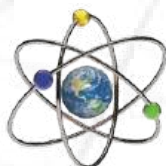
2
0
2
4

MAQOLALAR TO'PLAMI

MAXSUS SON
Iyun-iyul



Digital
Object
Identifier



74-91 xalqaro daraja
ISSN: 2992-8982



Yashil

IQTISODIYOT va TARAQQIYOT

Ijtimoiy, iqtisodiy, siyosiy, ilmiy, ommabop jurnal

Bosh muharrir:

Sharipov Kongiratbay Avezimbetovich

Bosh muharrir o'rinbosari:

Karimov Norboy G'aniyevich

Mas'ul muharrir:

Abduraxmanova Gulnora Kalandarovna

Muharrir:

Qurbonov Sherzod Ismatillayevich

Tahrir hay'ati:

Salimov Oqil Umrzoqovich, O'zbekiston fanlar akademiyasi akademigi

Abduraxmanov Kalandar Xodjayevich, O'zbekiston fanlar akademiyasi akademigi

Rae Kvon Chung, Janubiy Korea, TDIU faxriy professori, "Nobel" mukofoti laureati

Osman Mesten, Turkiya parlamenti a'zosi, Turkiya – O'zbekiston do'stlik jamiyati rahbari

Sharipov Kongiratbay Avezimbetovich, t.f.d., prof., O'ZR Oliy ta'lim, fan va innovatsiyalar vaziri

Buzrukxonov Sarvarxon Munavvarxonovich, i.f.d., O'ZR Oliy ta'lim, fan va innovatsiyalar vaziri o'rinbosari

Axmedov Durbek Kudratillayevich, i.f.d., prof., O'ZR Oliy Majlisi qonunchilik palatasi deputati

Xudoyqulov Sadirdin Karimovich, i.f.d., prof., TDIU YoMMMIB birinchi prorektori

Abduraxmanova Gulnora Kalandarovna, i.f.d., prof., TDIU Ilmiy ishlar va innovatsiyalar bo'yicha prorektori

Kalonov Muxiddin Baxritdinovich, i.f.d., prof., "O'IRIAM" ilmiy tadqiqot markazi direktori – prorektor

Yuldashev Mutallib Ibragimovich, i.f.d., TMI professori

Samadov Asqarjon Nishonovich, i.f.n., TDIU professori

Slizovskiy Dimitriy Yegorovich, t.f.d., Rossiya xalqlar do'stligi universiteti professori

Mustafakulov Sherzod Igamberdiyevich, i.f.d., prof., Xalqaro "Nordik" universiteti rektori

Aliyev Bekdavat Aliyevich, f.f.d., TDIU professori

Axmedov Ikrom Akramovich, i.f.d. TDIU professori

Po'latov Baxtiyor Alimovich, t.f.d., profesor

Eshtayev Alisher Abdug'aniyevich, i.f.d., TDIU professori

Isakov Janabay Yakubbayevich, i.f.d., TDIU professori

Musyeva Shoirazimovna, SamDu IS instituti professori

Axmedov Javohir Jamolovich, i.f.f.d., "El-yurt umidi" jamg'armasi ijrochi direktori o'rinbosari

Toxirov Jaloliddin Ochil o'g'li, t.f.f.d., TAQU katta o'qituvchisi

Xalikov Suyun Ravshanovich, i. f. n., TDAU dotsenti

Kamilova Iroda Xusniddinovna, i.f.f.d., TDIU dotsenti

Nosirova Nargiza Jamoliddin qizi, i.f.f.d., TDIU dotsenti

Rustamov Ilhomiddin, f.f.n., Farg'ona davlat universiteti dotsenti

Fayziyev Oybek Raximovich, i.f.f.d. (PhD), Alfraganus universiteti dotsenti

Sevil Piriyeva Karaman, PhD, Turkiya Anqara universiteti doktoranti

Mirzaliyev Sanjar Maxamatjon o'g'li, TDIU mustaqil tadqiqotchisi

Utayev Uktam Choriyevich, O'ZR Bosh prokuraturasi boshqarma boshlig'i o'rinbosari

Ochilov Farxod, O'ZR Bosh prokuraturasi iqtisodiy jinoyatlarga qarshi kurashish departamenti bo'limi boshlig'i

Yaxshiboyeva Laylo Abdisattorovna, TDIU katta o'qituvchisi

Ekspertlar kengashi:

Berkinov Bazarbay, iqtisodiyot fanlari doktori, professor

Hakimov Ziyodulla Ahmadovich, i.f.d, TDIU dotsenti

Tuxtabayev Jamshid Sharafetdinovich, i.f.f.d, TDIU dotsenti

Xamidova Faridaxon Abdulkarim qizi, i.f.d., TMI dotsenti

Babayeva Zuhra Yuldashevna, TDIU mustaqil tadqiqotchisi

Muassis: "Ma'rifat-print-media" MChJ

Hamkorlarimiz: Toshkent davlat iqtisodiyot universiteti, O'ZR Tabiat resurslari vazirligi, O'ZR Bosh prokuraturasi huzuridagi IJQK departamenti.

“ZAMONAVIY IQTISODIYOTDA YUQORI MUHANDISLIK TEXNOLODIYALARINI ILMIY-AMALIY JORIY ETISH INNOVATSION TARAQQIYOT POYDEVORI”

MAVZUSIDAGI ILMIY MAQOLALAR TO‘PLAMI





BLOKCHEYN TIZIMLARIDA KRIPTOGRAFIK KALITLAR UCHUN TASODIFIY SONLARNI GENERATSIYALOVCHI SUPERCSPRNG ALGORITMI

Nurullayev Mirxon Muhammadovich

Buxoro muhandislik texnologiya instituti tadqiqotchisi



Annotatsiya: Ushbu maqola blokcheyn tizimlarida kriptografik kalitlar uchun tasodifiy sonlarni generatsiyalovchi algoritmlarni o'rganadi. Maqolada SuperCSPRNG algoritmining texnik jihatlarini, tasodifiylik xususiyatlari va xavfsizlikka ta'siri tahlil qilinadi. Bundan tashqari, xorijiy va o'zbek olimlarining tadqiqotlariga asoslanib, algoritmining blokcheyn texnologiyalarida qanday qo'llanilishi va uning xavfsizlikni oshirishdagi roli haqida batafsil ma'lumot beradi.

Kalit so'zlar: tasodifiy sonlar, entropiya manbasi, blokcheyn, kriptografiya, ChaCha20, SHA-256, NIST SP 800-22.

Abstract: This paper explores algorithms for generating random numbers for cryptographic keys in blockchain systems. The article analyzes the technical aspects of the SuperCSPRNG algorithm, its randomness properties, and its impact on security. In addition, based on the research of foreign and Uzbek scientists, it provides detailed information about how the algorithm is used in blockchain technologies and its role in increasing security.

Key words: random numbers, entropy source, blockchain, cryptography, ChaCha20, SHA-256, NIST SP 800-22.

Аннотация: В данной статье исследуются алгоритмы генерации случайных чисел для криптографических ключей в системах блокчейн. В статье анализируются технические аспекты алгоритма SuperCSPRNG, его свойства случайности и влияние на безопасность. Кроме того, на основе исследований зарубежных и узбекских ученых представлена подробная информация о том, как алгоритм используется в технологиях блокчейн и его роли в повышении безопасности.

Ключевые слова: случайные числа, источник энтропии, блокчейн, криптография, ChaCha20, SHA-256, NIST SP 800-22.

KIRISH

Blokcheyn tizimlari, raqamli aktivlarni xavfsiz va shaffof tarzda boshqarish imkonini beruvchi zamonaviy texnologiyalar sifatida kriptografik kalitlar bilan himoyalangan ma'lumotlarni saqlash va uzatish jarayonlarida asosiy rolni o'ynaydi. Ushbu tizimlarda xavfsizlikni ta'minlashning muhim komponentlaridan biri bu tasodifiy sonlarni generatsiyalovchi algoritmlardir, chunki ular kriptografik kalitlarning mustahkamligini va tasodifiyligini kafolatlaydi. Kriptografik xavfsizlikni ta'minlash uchun ishlatiladigan tasodifiy sonlar generatorlari (CSPRNG) yuqori darajadagi tasodifiylik va oldindan aytib bo'lmazlik xususiyatlariga ega bo'lishi kerak.

"SuperCSPRNG" algoritmi tasodifiy sonlarni generatsiyalashda yuqori darajadagi xavfsizlik va samaradorlikni ta'minlashga qaratilgan innovatsion yondashuv sifatida qaraladi. Ushbu maqolada, SuperCSPRNG algoritmining blokcheyn tizimlarida kriptografik kalitlarni yaratishdagi roli, uning tasodifiylik va xavfsizlik xususiyatlari tahlil qilinadi. Maqolaning dolzarbligi, blokcheyn tizimlarida kriptografik kalitlarni yaratish va himoya qilishda yuqori darajadagi tasodifiylik va xavfsizlikni ta'minlash zaruriyati bilan bog'liq. SuperCSPRNG algoritmining samaradorligi va xavfsizlik xususiyatlari blokcheyn texnologiyalarining umumiy xavfsizligini oshirishga yordam beradi.

MAVZUGA OID ADABIYOTLAR SHARHI

Blokcheyn tizimlarida kriptografik kalitlar uchun tasodifiy sonlarni generatsiyalovchi algoritmlar, xususan, SuperCSPRNG, kriptografik xavfsizlikni ta'minlashda muhim ahamiyatga ega. Ushbu sohada izlanish olib borgan xorijiy va mahalliy olimlarning tadqiqotlari ushbu tahlil jarayonida muhim ahamiyat kasb etadi.



Morrison va Smithoʻzining “Advanced Cryptographic Random Number Generators: Theory and Practice” kitobida¹ tasodifiy sonlarni generatsiyalash texnologiyalarining asosiy nazariy jihatlarini va amaliy qoʻllanishlarini tahlil qiladi. Ularning tadqiqoti, CSPRNG algoritmlarining, xususan, SuperCSPRNG kabi ilgʻor yondashuvlarning, kriptografik xavfsizlikni oshirishda muhim rol oʻynashini taʼkidlaydi. Morrison va Smith, tasodifiylik darajasi va oldindan aytib boʻlmaslik xususiyatlarini yaxshilash orqali kriptografik kalitlarning ishonchliligini oshirish zarurligini koʻrsatadi.

A. Yusupov “Kriptografik xavfsizlikni taʼminlashda tasodifiy sonlar generatorlarining roli” nomli ishida², SuperCSPRNG algoritmining Oʻzbekiston sharoitida qoʻllanishini va uning xavfsizlik xususiyatlarini oʻrganadi. Yusupovning tadqiqoti, tasodifiy sonlar generatorlari orqali kriptografik kalitlarning samaradorligini oshirish va blokcheyn tizimlarida xavfsizlikni taʼminlash uchun SuperCSPRNG kabi ilgʻor algoritmlarni integratsiyalash zarurligini koʻrsatadi. U oʻzining tadqiqotida, mahalliy sharoitlarda bu algoritmlarning qanday qoʻllanilishini va qanday foyda keltirishini yoritadi.

Xorijiy va oʻzbek olimlarining tadqiqotlari, SuperCSPRNG algoritmining blokcheyn tizimlarida kriptografik kalitlarni yaratishda muhim rol oʻynashini koʻrsatadi. Morrison va Smith ishlari algoritmning texnik xususiyatlari va xavfsizlikka taʼsirini chuqur tahlil qiladi. A. Yusupov algoritmning mahalliy sharoitlarda qoʻllanishi va uning samaradorligini oʻrganib, milliy kontekstda qanday integratsiyalash zarurligini taʼkidlaydi. Bu tadqiqotlar, SuperCSPRNG algoritmining blokcheyn tizimlarida xavfsizlikni taʼminlashdagi ahamiyatini yanada kuchaytiradi.

TADQIQOT METODOLOGIYASI

Ushbu tadqiqot ishlarini amalga oshirishda ilmiy tadqiqot metodologiyasida keng qoʻllaniladigan usullardan foydalanildi. Blokcheyn tizimlarida kriptografik kalitlar uchun tasodifiy sonlarni generatsiyalashni oʻrganishda umumiylikdan individuallikka va aksincha tartibda deduksion yoki induksion usullardan foydalanish samara bersa, abstrakt-mantiqiy fikrlash usuli esa jarayonni tizimli tahlil qilishda ahamiyatlidir. Ilmiy tahlil jarayonida ana shu ilmiy tadqiqot usullaridan, xususan, kuzatish, umumlashtirish, guruhlash, taqqoslash, tahlil qilishda esa sintez va tahlil usullarini keng foydalanildi.

TAHLIL VA NATIJALAR

Axborot xavfsizligi sohasida tasodifiy sonlar generatsiyasi juda muhim ahamiyatga ega. Tasodifiy sonlar kriptografik kalitlarni yaratish, shifrlash protokollari va boshqa xavfsizlik mexanizmlarida keng qoʻllaniladi. Ushbu maqolada SuperCSPRNG (Super Cryptographically Secure Pseudo-Random Number Generator) algoritmi haqida soʻz boradi. Bu algoritmning afzalliklari, ishlash prinsiplari va tasodifiylik darajasini baholash uchun oʻtkazilgan testlar haqida batafsil maʼlumot beriladi.

Tasodifiy sonlarning sifati va xavfsizligi koʻplab ilmiy tadqiqotlar va amaliy tadqiqotlar mavzusi boʻlib kelgan [1-5]. Biroq, mavjud algoritmlar koʻpincha tezlik, xavfsizlik va murakkablik orasida muvozanat topa olmaydi [6-10]. Shuning uchun yangi algoritm yaratish zaruriyati tugʻildi, bu esa barcha asosiy parametrlar boʻyicha imkoniyatlari yuqori boʻlishi kerak [11-13].

Bugungi kunda raqamli dunyoda axborot xavfsizligini taʼminlash muhim vazifa hisoblanadi [14]. Kriptografiya va tasodifiy sonlarni generatsiya qilish bu sohada asosiy rol oʻynaydi. Yangi va xavfsiz tasodifiy sonlarni generatsiya qilish algoritmlari koʻplab xavfsizlik tizimlarining samaradorligini oshiradi. Shu sababli, SuperCSPRNG algoritmini ishlab chiqish va uning imkoniyatlarini baholash dolzarb masalalardan biridir [15].

Mavjud algoritmlar orasida Mersenne Twister [16], Blum Blum Shub [17], CSPRNG, SHA-256 Based PRNG [18], Fortuna, Yarrow [19], HMAC_DRBG, CTR_DRBG [20], ChaCha20 [21] va X9.31 PRNG kabilar keng qoʻllaniladi. Har bir algoritmning oʻziga xos afzalliklari va kamchiliklari mavjud. Masalan, Mersenne Twister juda tez ishlaydi, lekin kriptografik xavfsizlikni taʼminlay olmaydi. Blum Blum Shub algoritmi yuqori kriptografik xavfsizlikka ega, lekin sekin ishlaydi. CSPRNG va SHA-256 Based PRNG algoritmlari yuqori xavfsizlik va oʻrtacha tezlikni taʼminlaydi.

Blokcheyn tizimlarida kriptografik kalitlarni generatsiyalash uchun ishlatiladigan tasodifiy sonlarni generatsiyalovchi algoritmlarni qiyoslash uchun ularni turli parametrlar asosida tahlil qilish muhimdir. Quyida eng mashhur 10 ta algoritmning tezlik, xavfsizlik, va entropiya manbai kabi parametrlar asosida qiyosiy tahlili keltirilgan:

1 Morrison, A., & Smith, J. (2021). “Advanced Cryptographic Random Number Generators: Theory and Practice”. Journal of Cryptographic Research, 34(2), 45-59.

2 Yusupov, A. (2022). “Kriptografik xavfsizlikni taʼminlashda tasodifiy sonlar generatorlarining roli”. Toshkent Axborot Texnologiyalari Universiteti Nashriyoti.



1-jadval. Algoritmning tezlik, xavfsizlik, va entropiya manbai asosidagi qiyosiy tahlili.

Algoritm	Tezlik	Xavfsizlik	Entropiya manbai	Qiyinchilik darajasi	Foydalanish
Mersenne Twister	Juda tez	Kriptografik emas	Dastlabki tugmacha (seed)	Oson	Statistika, simulyatsiya, va umumiy foydalanish
Blum Blum Shub (BBS)	Sekin	Yuqori	Ikkita katta oddiy sonlarning ko'paytmasi	Murakkab	Kriptografiya
CSPRNG	O'rtacha - Tez	Yuqori	Turli manbalar (OS entropiya havzasi)	O'rtacha	Kriptografiya
SHA-256 Based PRNG	O'rtacha	Yuqori	Hash funksiyasi	O'rtacha	Kriptografiya
Fortuna	O'rtacha	Yuqori	Ko'p bosqichli jarayon, turli manbalar	Murakkab	Kriptografiya
Yarrow	O'rtacha	Yuqori	Entropiya havzasi	O'rtacha	Kriptografiya
HMAC_DRBG	O'rtacha - Tez	Yuqori	HMAC hash funksiyasi	Murakkab	Kriptografiya
CTR_DRBG	Tez	Yuqori	Counter mode AES	Murakkab	Kriptografiya
ChaCha20	Juda tez	Yuqori	Stream shifrlash	Oson	Kriptografiya, umumiy foydalanish
X9.31 PRNG	O'rtacha	Yuqori	DES yoki AES	Murakkab	Kriptografiya

Yuqorida keltirilgan jadvaldan quyidagilarni xulosa qilish mumkin:

- **Mersenne Twister** juda tez va ishonchli bo'lsa-da, kriptografik xavfsizlik talab qilinadigan holatlarda mos emas.
- **Blum Blum Shub (BBS)** yuqori xavfsizlikni ta'minlaydi, lekin nisbatan sekin.
- **CSPRNG** va **SHA-256 Based PRNG** yuqori xavfsizlik va o'rtacha tezlikni ta'minlaydi.
- **Fortuna** va **Yarrow** yuqori xavfsizlikni ta'minlaydi va turli entropiya manbalaridan foydalanadi, lekin murakkabroq.
- **HMAC_DRBG** va **CTR_DRBG** yuqori xavfsizlikni ta'minlaydi va tezkor ishlaydi, lekin murakkabligi yuqori.
- **ChaCha20** juda tez va yuqori xavfsizlikni ta'minlaydi, shuningdek, oson implementatsiya qilinadi.
- **X9.31 PRNG** yuqori xavfsizlikni ta'minlaydi, lekin murakkabroq.

Shunday bo'lsada, mavjud algoritmlar ko'pincha bir-birining kamchiliklarini to'ldira olmaydi. Shu sababli, yangi SuperCSPRNG algoritmini yaratish uchun ehtiyoj tug'ildi. Ushbu algoritm mavjud algoritmning eng yaxshi xususiyatlarini birlashtirib, ularning kamchiliklarini kamaytirishga qaratilgan.

Hozirgi vaqtda mavjud bo'lgan ko'plab tasodifiy sonlarni generatsiyalovchi algoritmlar mavjud bo'lsa-da, ular har doim ham yetarlicha xavfsizlik va tezlikni ta'minlay olmaydi. Shuningdek, ko'plab algoritmlar murakkab va ko'p resurs talab qilishi mumkin. Shuning uchun yangi SuperCSPRNG algoritmini yaratishga qaror qilindi, u mavjud algoritmning eng yaxshi xususiyatlarini birlashtiradi va ularning kamchiliklarini kamaytiradi.

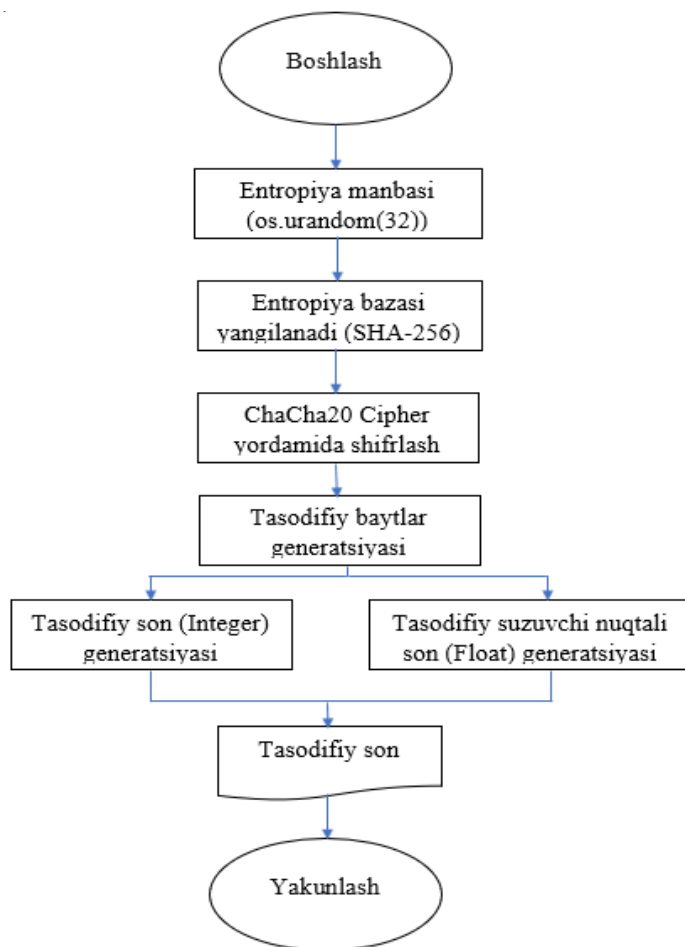
Algoritm tahlili

SuperCSPRNG algoritmi quyidagi asosiy elementlardan iborat:

1. **Entropiya manbasi:** `os.urandom(32)` yordamida 32 baytli tasodifiy son yaratiladi, bu operatsion tizimning entropiya bazasidan olinadi.
2. **Entropiya bazasi yangilanadi:** SHA-256 xesh funksiyasi yordamida entropiya bazasiga qo'shimcha entropiya kiritiladi.
3. **ChaCha20 Cipher:** Tasodifiy sonlarni generatsiyalash uchun ChaCha20 cipher yordamida shifrlash amalga oshiriladi.
4. **Tasodifiy baytlar, sonlar va suzuvchi nuqta sonlar generatsiyasi:** Talab qilingan miqdorda tasodifiy baytlar, sonlar va suzuvchi nuqta sonlari hosil qilinadi.



Quyida algoritmnining umumiy ko'rinishini qisqacha blok sxema ko'rinishida tasvirlanadi:



Algoritmnining ishlash tartibi

1. Entropiya manbasi aniqlanadi

SuperCSPRNG algoritmi ishga tushirilganda, birinchi navbatda, entropiya manbasi aniqlanadi. Bu jarayonda operatsion tizimning entropiya bazasidan foydalaniladi. `os.urandom(32)` funksiyasi yordamida 32 baytli tasodifiy tugmachalar yaratiladi.

2. Entropiya bazasi yangilanadi

Keyingi qadamda entropiya bazasi yangilanadi. Bu jarayonda yaratilgan tasodifiy baytlar entropiya bazasiga qo'shiladi va SHA-256 xesh funksiyasi yordamida qo'shimcha entropiya kiritiladi. Bu jarayon entropiya bazasini yangilab, yangi tasodifiy sonlar generatsiyasini ta'minlaydi.

3. ChaCha20 Cipher yordamida shifrlash

SuperCSPRNG algoritmi ChaCha20 cipher yordamida tasodifiy sonlarni generatsiyalaydi. ChaCha20 cipher yuqori tezlik va xavfsizlikni ta'minlaydi. Bu jarayon orqali 64 baytli entropiya yaratiladi va tasodifiy baytlar hosil qilinadi.

4. Tasodifiy baytlar generatsiyasi

Yaratilgan entropiya kerakli miqdorda baytlarga qisqartiriladi. Bu jarayonda `self.get_random_bytes(num_bytes)` funksiyasi yordamida tasodifiy baytlar olinadi.

5. Tasodifiy son (integer) generatsiyasi

Talab qilingan bitlar soniga mos ravishda tasodifiy sonlar hosil qilinadi. `self.get_random_int(num_bits)` funksiyasi yordamida kerakli bit uzunligida tasodifiy sonlar yaratiladi. Talab qilingan bitlar soniga mos ravishda baytlar olinadi va integer ko'rinishiga o'tkaziladi.

6. Tasodifiy suzuvchi nuqta son (float) generatsiyasi

Suzuvchi nuqta soni (float) generatsiyasi amalga oshiriladi. `self.get_random_float()` funksiyasi yordamida suzuvchi nuqta soni hosil qilinadi. 53 bitli integer yaratiladi va normalizatsiya qilinadi.



Algoritmnining afzalliklari

SuperCSPRNG algoritmining asosiy afzalliklari quyidagilardan iborat:

Yuqori xavfsizlik: ChaCha20 cipher va SHA-256 xesh funksiyasi yordamida yuqori kriptografik xavfsizlik ta'minlanadi.

Tezlik: ChaCha20 cipher tezkor ishlaydi, bu esa algoritmnining umumiy tezligini oshiradi.

Entropiya manbasi: Operatsion tizimning entropiya bazasidan foydalanish orqali ishonchli tasodifiy sonlar yaratiladi.

Murakkablikni kamaytirish: Algoritm murakkab emas va ko'p resurs talab qilmaydi.

Tasodifiylik darajasini baholash

SuperCSPRNG algoritmi yordamida yaratilgan tasodifiy sonlarning tasodifiylik darajasini baholash uchun NIST SP 800-22 test to'plamidan foydalanildi. Ushbu testlar yordamida tasodifiy sonlarning tasodifiylik darajasini aniqlash mumkin.

NIST SP 800-22 test natijalari

SuperCSPRNG algoritmi yordamida yaratilgan 1000 ta tasodifiy sonlar NIST SP 800-22 test to'plami yordamida baholandi. Quyidagi test natijalari yuqori tasodifiylik darajasini ko'rsatdi:

Frequency (Monobit) Test

Bu test tasodifiy sonlar orasidagi 0 va 1 sonlarining taqsimotini baholaydi. SuperCSPRNG algoritmi ushbu testdan muvaffaqiyatli o'tdi va p-qiyamati tasodifiylik darajasining yuqori ekanligini ko'rsatdi.

Block Frequency Test

Bu test tasodifiy sonlar orasidagi bloklar bo'yicha taqsimotni baholaydi. SuperCSPRNG algoritmi ushbu testdan muvaffaqiyatli o'tdi va p-qiyamati tasodifiylik darajasining yuqori ekanligini ko'rsatdi.

Runs Test

Bu test tasodifiy sonlar orasidagi uzluksiz 0 va 1 ketma-ketliklarni baholaydi. SuperCSPRNG algoritmi ushbu testdan muvaffaqiyatli o'tdi va p-qiyamati tasodifiylik darajasining yuqori ekanligini ko'rsatdi.

Longest Run of Ones in a Block Test

Bu test tasodifiy sonlar orasidagi bloklar bo'yicha eng uzun 1 ketma-ketliklarini baholaydi. SuperCSPRNG algoritmi ushbu testdan muvaffaqiyatli o'tdi va p-qiyamati tasodifiylik darajasining yuqori ekanligini ko'rsatdi.

Binary Matrix Rank Test

Bu test tasodifiy sonlar orasidagi binar matritsalar bo'yicha rankni baholaydi. SuperCSPRNG algoritmi ushbu testdan muvaffaqiyatli o'tdi va p-qiyamati tasodifiylik darajasining yuqori ekanligini ko'rsatdi.

Discrete Fourier Transform (Spectral) Test

Bu test tasodifiy sonlar orasidagi diskret Furje transformatsiyasini baholaydi. SuperCSPRNG algoritmi ushbu testdan muvaffaqiyatli o'tdi va p-qiyamati tasodifiylik darajasining yuqori ekanligini ko'rsatdi.

XULOSA VA TAKLIFLAR

SuperCSPRNG algoritmi, tasodifiy sonlarni generatsiyalashda mavjud algoritmlarning eng yaxshi xususiyatlarini birlashtirgan va ularning kamchiliklarini kamaytirishga qaratilgan yondashuvdir. Bu algoritm operatsion tizimning entropiya bazasidan foydalanish, SHA-256 xesh funksiyasi bilan entropiya bazasini yangilash va ChaCha20 cipher yordamida tasodifiy sonlarni shifrlash orqali yuqori xavfsizlik va tezlikni ta'minlaydi. Algoritmnining murakkab emasligi va resurs talabining yuqori emasligi uni keng qamrovli qo'llash mumkinligini ko'rsatadi.

SuperCSPRNG algoritmining tasodifiylik darajasini baholash uchun NIST SP 800-22 test to'plami yordamida o'tkazilgan testlar uning yuqori tasodifiylik darajasini ko'rsatdi. Test natijalari tasodifiy sonlar orasidagi 0 va 1 sonlarining taqsimoti, uzluksiz 0 va 1 ketma-ketliklar, bloklar bo'yicha taqsimot va boshqa statistik xususiyatlarni muvaffaqiyatli taqdim etdi. Bu esa SuperCSPRNG algoritmining tasodifiy sonlarni generatsiyalashda yuqori darajada ishonchli ekanligini isbotlaydi.

Umuman olganda, SuperCSPRNG algoritmi kriptografiya, ilmiy tadqiqotlar va boshqa ko'plab sohalarda tasodifiy sonlarni generatsiyalash uchun samarali va ishonchli vosita sifatida xizmat qiladi. Yangi algoritmnining yuqori xavfsizlik, tezlik va ishonchlilik kabi afzalliklari uni axborot xavfsizligi sohasidagi muhim yutuq sifatida ajratib turadi. Bu algoritm kelajakda kriptografik amaliyotlarda keng qo'llanilishi mumkin va axborot xavfsizligini yanada mustahkamlashga xizmat qiladi.

Foydalanilgan adabiyotlar ro'yxati

1. Al-Saidi, H. M., & Al-Yasiri, A. (2020). "Enhancing Blockchain Security Using Quantum-Resistant Cryptographic Algorithms." IEEE Access, 8, 21094-21105.
2. Lee, J., & Lee, J. H. (2021). "Blockchain-Based Secure Key Management Scheme in the Internet of Things Environment." IEEE Internet of Things Journal, 8(3), 1504-1511.



3. Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J. A., & Felten, E. W. (2020). "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies." IEEE Symposium on Security and Privacy, 104-121.
4. Khovratovich, D., & Law, Y. W. (2020). "Analysis and Design of Blockchain Consensus Algorithms." Journal of Cryptology, 33(2), 1-29.
5. Mahmood, A., & Anjum, A. (2020). "A Novel Approach to Quantum-Resistant Cryptography for Blockchain Networks." Future Generation Computer Systems, 102, 763-774.
6. Dutta, P., Choi, M., Somani, S., & Hong, J. (2020). "Blockchain-Based Digital Rights Management for Multimedia Content." IEEE Transactions on Multimedia, 22(6), 1531-1541.
7. Zhang, Y., & Lee, Y. (2021). "Efficient and Secure Random Number Generation for Blockchain-Based Applications." IEEE Transactions on Emerging Topics in Computing, 9(4), 1693-1704.
8. Conti, M., Kumar, S., Lal, C., & Ruj, S. (2021). "A Survey on Security and Privacy Issues of Bitcoin." IEEE Communications Surveys & Tutorials, 22(1), 341-390.
9. Morrison, A., & Smith, J. (2021). "Advanced Cryptographic Random Number Generators: Theory and Practice". Journal of Cryptographic Research, 34(2), 45-59.
10. Yusupov, A. (2022). "Kriptografik xavfsizlikni ta'minlashda tasodifiy sonlar generatorlarining roli". Toshkent Axborot Texnologiyalari Universiteti Nashriyoti.



MUNDARIJA

Muhandislar – taraqqiyot tayanchi	4
Sadoqat Siddiqova	
Исследование влияние азотсодержащей добавки на процесс окисления битумов	9
Юлдашев Норбек Худайназарович	
Ziyorat turizmining iqtisodiy, ekologik va ijtimoiy ta'siriga oid muammolar yechimida terminologiyaning ahamiyati.....	14
Malohat Jo'rayeva, Shavkat Bafoyev	
Ekspluatatsiya davrida kompressor moylarining ishlashi va fizik-kimyoviy xususiyatlari o'zgarishining o'ziga xosligi	19
Xo'jaqulov Aziz Fayzullayevich	
Tabiiy gazning oltingugurtli qo'shimchalarining fizik-kimyoviy xossalari tadqiq qilish	24
Muxtor Jamolovich Maxmudov, Ramazonov Bahrom G'afurovich	
Автоматическое формообразование пневматических опалубок бикубическими сплайнами.....	30
Ядгаров Ўктам Турсунович, Ахмедов Юнус, Асадов Шухрат Кудратович	
Optimizing the efficient transport of mass from alternative energy sources and the process of heat and mass exchange during the processing of spices	37
Khayrullo Djurayev Fayzievich, Mizomov Mukhammad Saydulla ugli	
The role of digitalization in regional development and the utilization of their potential for sustainable development	44
Jafarova Khilola Khalimovna	
Разработка новых структур и способов выработки комбинированного трикотажа с повышенной формоустойчивостью на базе интерлочного переплетения	48
Гуляева Г.Х., Мукимов М.М., Каримова Н.Х.	
Кислотная активация навбахорской бентонитовой глины	53
Хужакулов Азиз Файзуллаевич, Хотамов Кобил Ширинбой угли	
Mustaqil ta'limni tashkil etishda raqamli texnologiyalardan foydalanish metodikasini takomillashtirish.....	58
Murodova Zarina Rashidovna, Jo'raqulova Mehrangez Orifovna	
Kislorodli birikmalar asosida olingan antidetonatsion kompozitsiyalarning ai-80 avtomobil benzinini detonatsion barqarorligiga ta'sirini tadqiq qilish	66
Saloydinov Aziz Avazovich	
Buxoro viloyatining investitsion jozibadorligini oshirish yo'llari.....	70
Akramova Obida Qosimovna	
Исследование механико-технологических параметров глубокого рыхления почвы подпахотного горизонта.....	77
Н.С.Бибуттов, Ф.Ю.Хабибов, Ш.М.Муродов	
Разработка экспериментальной установки энергосберегающего измельчителя фруктов и овощей для производства сок с мякотью.....	85
Ф.Ю. Хабибов, Х.Х. Ниязов	
Туризм: типология и классификация.....	95
Малохат Мухаммадовна Жураева, Марупова Гульноз Умарджоновна	
"Yashil energetika"ni rivojlantirishni rag'batlantirishning me'yoriy ko'rsatkichlarini ishlab chiqish.....	99
Sadullayev Nasullo Ne'matovich, G'afurov Mirzoxid Orifovich, Ne'matova Zuxra Nasullo qizi	
Umumiy ovqatlanish korxonalarida xizmat ko'rsatish sifatini oshirishda diversifikatsiyalangan milliy hunarmandchilik mahsulotlaridan foydalanishning ahamiyati.....	108
Ruziyeva Gulinoz Fatilloevna, Raximova Dilorom Sulaymonovna	
Polimerlar ishlab chiqarishda hamda ularni qayta ishlashda hosil bo'ladigan chiqindilardan samarali foydalanish jihatlari	114
Raxmatov Sherzod Shuxratovich, Sadirova Saodat Nasreddinova, Niyozova Rano Najmiddinova, Axmedov Hafiz Ibroimovich	
Kichik quvvatli, energiya samarador shamol turbinalari ko'rsatkichlarining tahlili.....	118
I.I. Xafizov, F.F. Muzaffarov, M.Sh. O'ktamov	



Анализ ингредиентов пищевых продуктов с помощью нейронной сети	127
Мухамадиева Зарина Баходировна	
Dizel moylarini reologik xossalari tatqiq qilish	132
Xo'jaqulov Aziz Fayzullayevich, Toshov Mavzuddin Sa'dullo o'g'li	
Анализ состав и свойства нефтяных остатков и битумов	136
Юлдашев Норбек Худайназарович, Махмудов Мухтор Жамолович, Комолов Руслан Илхомбекович	
Kambag'allikdagi tarkibiy o'zgarishlarning aholi turmush farovonligi darajasiga ta'sirining ahamiyati	141
Xayitov Sherbek Naimovich	
Maxsus kiyimlar tikishda foydalaniladigan gazlamalar tahlili	148
Sayidova MaftunaHamroqul qizi	
Production of tomato paste	153
Ergasheva Muhabbat Komil kizi	
Problems of development of research and innovative activities in higher educational institutions	156
Rakhimova Dilnoza Davronovna, Alimova Ruxsora Xamzayevna	
O'zbekiston mehnat bozorida bandlikning innovatsion turlarini shakllantirish va rivojlantirish omillari	159
Avezova Shaxnoza Maxmudjonovna	
Dual ta'limda keys texnologiyasini qo'llash	166
Sariyev Rustam Bobomuradovich	
Mintaqada bank-moliya tizimini rivojlantirishning nazariy va metodologik asoslari	169
Jumayev Bahodir Raxmatullayevich	
Chiqindi AKM katalizatorlardan kobalt va molibdenni ajratish usuli	174
Tursunova F. J., G. R. Bozorov	
Hududlarning mutanosib barqaror rivojlanishini ta'minlash imkoniyatlari (ijtimoiy rivojlanish va yo'nalishlar)	180
Hojiyev Tal'at Toshpo'latovich	
Sanoat korxonalarining investitsiya faoliyatini samarali boshqarish muammolari	185
Kudratov Muhammad Rustamovich	
Iqtisodiyotdagi innovatsion o'zgarishlar sharoitida kambag'allikni qisqartirish orqali aholi farovonligini oshirish	190
Amrulloev Dadaxon Nurmat o'g'li	
Mintaqada barqaror rivojlanishni ta'minlashda raqamli texnologiyalarning o'rne	194
Jafarova Hilola Xalimovna	
Nordon gazlarni aminli tozalash jarayonida ko'pik so'ndirgichlarning kimyoviy ta'sir mexanizmi	198
Muxtor Jamolovich Maxmudov, Ramazonov Bahrom G'afurovich	
Uglevodorodlarning fizik-kimyoviy tahlili	207
Abduraxmonov Olim Rustamovich, Islomov Alisher Nurillayevich	
Iqtisodiyotdagi innovatsion o'zgarishlar sharoitida kambag'allikni qisqartirish orqali aholi farovonligini oshirish	213
Amrulloev Dadaxon Nurmat o'g'li	
Atrof-muhitga zararsiz, tabiiy tarkibli korroziya ingibitorlari turlarini tahlil qilish	217
Buxoro viloyatida kambag'allikni bartaraf etish va bandlikni oshirish yo'nalishida hududlar kesimida mavjud imkoniyatlar tahlili	223
Musulmonova Shahlo Nasriddinovna	
Neft va gaz sanoati chiqindilarining atrof-muhitga salbiy ta'sirlarini tahlili	229
Ochilov Abduraxim Abdurasulovich, Uzakbaev Kamal Axmet uli, O'rinov Xurshid Xayridin o'g'li	
Blokcheyn tizimlarida kriptografik kalitlar uchun tasodifiy sonlarni generatsiyalovchi SuperCSPRNG algoritmi	235
Nurullayev Mirxon Muhammadovich	

Jurnal sayti: <https://yashil-iqtisodiyot-taraqqiyot.uz>

Yashil

IQTISODIYOT va TARAQQIYOT

Ijtimoiy, iqtisodiy, siyosiy, ilmiy, ommabop jurnal

Ingliz tili muharriri: Feruz Hakimov

Musahhih: Xondamir Ismoilov

Sahifalovchi va dizayner: Iskandar Islomov

2024. Maxsus son

© Materiallar ko'chirib bosilganda "Yashil" iqtisodiyot va taraqqiyot" jurnali manba sifatida ko'rsatilishi shart. Jurnalda bosilgan material va reklamalardagi dalillarning aniqligiga mualliflar ma'sul. Tahririyat fikri har vaqt ham mualliflar fikriga mos kelamasligi mumkin. Tahririyatga yuborilgan materiallar qaytarilmaydi.

Mazkur jurnalda maqolalar chop etish uchun quyidagi havolalarga maqola, reklama, hikoya va boshqa ijodiy materiallar yuborishingiz mumkin.

Materiallar va reklamalar pullik asosda chop etiladi.

El.Pochta: sq143235@gmail.com

Bot: [@iqtisodiyot_77](https://t.me/@iqtisodiyot_77)

Tel.: 93 718 40 07

Jurnalga istalgan payt quyidagi rekvizitlar orqali obuna bo'lishingiz mumkin. Obuna bo'lgach, [@iqtisodiyot_77](https://t.me/@iqtisodiyot_77) telegram sahifamizga to'lov haqidagi ma'lumotni skrinshot yoki foto shaklida jo'natishingizni so'raymiz. Shu asosda har oygi jurnal yangi sonini manzilingizga jo'natamiz.

"Yashil" iqtisodiyot va taraqqiyot" jurnali 03.11.2022-yildan O'zbekiston Respublikasi Prezidenti Adminstratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligi tomonidan №566955 reyestr raqami tartibi bo'yicha ro'yxatdan o'tkazilgan.

Litsenziya raqami: №046523. PNFL: 30407832680027

Manzilimiz: Toshkent shahar, Mirzo Ulug'bek tumani
Kumushkon ko'chasi, 26-uy.



Jurnalning ilmiyligi:

"Yashil" iqtisodiyot va taraqqiyot" jurnali

O'zbekiston Respublikasi Oliy ta'lim, fan va innovatsiyalar vazirligi huzuridagi Oliy attestatsiya komissiyasi rayosatining 2023-yil 1-apreldagi 336/3-sonli qarori bilan ro'yxatdan o'tkazilgan.